Senatsverwaltung für Inneres und Sport



Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin

(Informationssicherheitsleitlinie – InfoSic-LL)

(Festsetzung vom 21.09.2017 gemäß **§ 21, Abs. 2 Satz 2 Nr. 4** EGovG Bln)

Version: 1.0.1

Stand: <7.8.17>

Inhaltsverzeichnis

1 Einleitung

In dieser Leitlinie zur Informationssicherheit (InfoSic-LL) werden für die vom Geltungsbereich des E-Government-Gesetzes Berlin – EGovG Bln erfassten Einrichtungen der Berliner Verwaltung die grundlegenden Ziele Anforderungen und die Strategie der Informationssicherheit sowie deren Organisationsstruktur festgelegt. Die Leitlinie zur Informationssicherheit

- beschreibt den Stellenwert der Informationssicherheit
- legt den Geltungsbereich fest
- legt die Sicherheitsstrategie fest
- formuliert die allgemeinen Sicherheitsziele
- definiert die Sicherheitsorganisation
- verpflichtet zur kontinuierlichen Fortschreibung des Regelwerks zur Informationssicherheit.

Die Leitlinie zur Informationssicherheit basiert auf den Regelungen des EGovG Bln. Sie ist Bestandteil der gemäß § 21, Abs. 2, Satz 2, Nr. 4 EGovG Bln festzusetzenden IKT-Sicherheitsarchitektur und ist das übergeordnete Regelwerk für die IKT-Sicherheit[1] in der Berliner Verwaltung.

Mit diesem Dokument wird für das Land Berlin auch der Beschluss des IT-Planungsrates vom 19.02.2013 in der Version 1.8 zur Erstellung einer Informationssicherheitsleitlinie umgesetzt.

Das vorliegende Dokument basiert weiterhin auf

- den Standards des Bundesamtes für Informationssicherheit (BSI) einschließlich der IT-Grundschutzkataloge
- dem Berliner Datenschutzgesetz (BlnDSG) bzw. - sofern zutreffend - Bundesdatenschutzgesetz und
- den internationalen Standards der ISO 2700x-Reihe.

2 Geltungsbereich

Diese Leitlinie zur Informationssicherheit ist das übergeordnete Regelwerk für das landesweite Informationssicherheitsmanagement im Land Berlin. Sie bildet die Grundlage für weitere Regelungen der IKT-Sicherheitsarchitektur sowie für behördenspezifische Regelungen. Sie gilt für alle vom Geltungsbereich des EGovG Bln erfassten Einrichtungen der Berliner Verwaltung und ist von diesen entsprechend ihrer Aufgabenverantwortung umzusetzen.

---

1 In Übereinstimmung mit dem Sprachgebrauch in nationalen und internationalen Standards wird – soweit sinnvoll und erforderlich – in der InfoSic-LL teilweise der Begriff IT-Sicherheit bzw. Informationssicherheit gleichrangig zum Begriff der IKT-Sicherheit verwendet.

Für Einrichtungen, die das vom ITDZ Berlin betriebene Berliner Landesnetz nutzen und nicht vom Geltungsbereich des EGovG Bln erfasst sind, gelten alle sich aus dieser Leitlinie und darauf aufbauenden Regelungen ergebenden Anforderungen an eine sichere Nutzung des Berliner Landesnetzes und sind von diesen umzusetzen.

Die Behörden der Berliner Verwaltung erstellen für ihre Bereiche ergänzende behördliche Informationssicherheitsleitlinien und setzen sie in ihrem Verantwortungsbereich – unter Beachtung der IKT-Sicherheitsarchitektur - eigenständig um.

3 Stellenwert der Informationssicherheit

Ziel der Informationssicherheit ist der angemessene Schutz der Informationen zur Bewahrung der verfassungsmäßigen Ordnung, zum Schutz des informationellen Selbstbestimmungsrechts und die Gewährleistung der Ordnungsmäßigkeit des Verwaltungshandelns, unabhängig davon, ob Informationen mit oder ohne Unterstützung von IKT verarbeitet werden.

Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt maßgeblich von den organisatorischen und personellen Rahmenbedingungen ab.

Eine funktionierende Verwaltung ist heute ohne IKT nicht mehr denkbar. Die Informationssicherheit nimmt daher in Zeiten der fortschreitenden elektronischen Datenverarbeitung, der zunehmenden Vernetzung sowie der steigenden Bedrohung durch Angriffe einen immer höheren Stellenwert ein:

- Dienstleistungen für Bürgerinnen und Bürger, Wirtschaft und Verwaltung und die internen Geschäftsprozesse der Berliner Behörden müssen sicher und rechtskonform erbracht werden.

- Die gesetzlichen Vorschriften, beispielsweise zum Datenschutz müssen eingehalten werden. Dienst- und Amtsgeheimnisse müssen gewahrt bleiben.

- Unbefugt veränderte oder gelöschte Daten können zu finanziellen Verlusten und evtl. zu Regressansprüchen führen. Die Verletzung der Sicherheitsziele kann zu deutlichen Ansehens- und Vertrauensverlusten führen. Ein Ausfall der IKT kann die Berliner Verwaltung in ihrer Arbeitsfähigkeit stark einschränken.

- Mögliche Schadensereignisse sind daher zu vermeiden bzw. deren Auswirkungen durch angemessene Vorsorgemaßnahmen zu minimieren.

- Die in IKT, Informationen, Geschäftsprozesse und Wissen investierten Werte müssen erhalten bleiben.

4 Verantwortung der Behördenleitung

Die Gewährleistung der Informationssicherheit gehört zum integralen Selbstverständnis der Berliner Verwaltung. Alle Leitungsebenen sind gehalten, ein vorbildliches Sicherheitsverhalten zu zeigen und motivierendes Vorbild für die Mitarbeiterinnen und Mitarbeiter zu sein.

Gemäß § 21, Abs. 2 Satz 2 Nr. 4 EGovG Bln verantwortet die IKT-Staatssekretärin oder der IKT-Staatssekretär die fortlaufende Weiterentwicklung und Festsetzung der zentralen IKT-Sicherheitsarchitektur und der Standards für die IKT-Sicherheit in der Berliner Verwaltung und deren Unterstützung und Überwachung bei der Umsetzung der IKT-Sicherheits-Standards

Die Leitungen der Behörden tragen die Verantwortung für die Informationssicherheit in ihren Zuständigkeitsbereichen auf der Grundlage des behördlichen Informations-Sicherheits-Management-System (ISMS) gemäß § 23 EGovG Bln.

Die jeweiligen Behördenleitungen verantworten die Steuerung und Aufrechterhaltung der Informationssicherheit, die Integration der Informationssicherheit in alle Geschäftsprozesse, das Risikomanagement (insbesondere die Festlegung sicherheitskritischer Geschäftsprozesse und Informationen sowie die Entscheidung über den Umgang mit Risiken) sowie die Verabschiedung der behördlichen Leitlinie zur Informationssicherheit innerhalb ihres Zuständigkeitsbereiches. Sie stellen ausreichend finanzielle und personelle Ressourcen zur Verfügung, um die erforderlichen infrastrukturellen, organisatorischen und technischen Maßnahmen umsetzen zu können. Sie sind verantwortlich für die Durchführung der erforderlichen Schulungs- und Sensibilisierungsmaßnahmen für alle Beschäftigten.

5 Festlegung von Sicherheitszielen

Zur Abbildung des hohen Stellenwertes der Informationssicherheit werden für die Berliner Verwaltung die nachstehenden Sicherheitsziele festgelegt, für die geeignete Sicherheitsniveaus definiert werden:

- **Vertraulichkeit**
  Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein[2].

  Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang (wer, wann, wie lange, mit wem etc.) sowie die Daten über den Sende- und Empfangsvorgang.

---

[2] (vgl. BSI Grundschutz-Katalog Nr. 4 - Glossar und Begriffsdefinitionen)

Im Prozess der Gestaltung und der Auswahl von Verfahren zur Verarbeitung personenbezogener Daten sind die zuständigen Datenschutzbeauftragten rechtzeitig einzubinden.

- **Integrität**
  Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten/Informationen und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf Daten/Informationen angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind[3].

  Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit (Unversehrtheit). Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Der Begriff Integrität bezieht sich auch auf die korrekte Funktionsweise von IKT-Systemen, da die Integrität der Informationen und Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden kann

- **Verfügbarkeit**
  Die Verfügbarkeit von Dienstleistungen, Funktionen der IKT oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können[4].

  Informationen, Dienstleistungen, Funktionen eines IKT-Systems haben der Anwenderin oder dem Anwender zum richtigen Zeitpunkt am richtigen Ort wie vorgesehen zur Verfügung zur stehen.

Für die Verarbeitung personenbezogener Daten werden aufgrund der erhöhten Anforderungen an den Datenschutz zusätzlich **Datenminimierung**, **Nichtverkettung, Intervenierbarkeit**, und **Transparenz** als Sicherheitsziele festgelegt:[5]

- **Datenminimierung**
  Planung, Gestaltung und Auswahl von IKT-Systemen haben sich an dem Ziel auszurichten, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks erforderlich ist. Von den Möglichkeiten der Anonymisierung und Pseudonymisierung ist Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

- **Nichtverkettung**
  Daten können nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden.

---

[3] Vgl. BSI Grundschutz-Katalog Nr. 4 - Glossar und Begriffsdefinitionen

[4] Vgl. BSI Grundschutz-Katalog Nr. 4 - Glossar und Begriffsdefinitionen

5 Vgl. hierzu: „Das Standard-Datenschutzmodell“ V.1.0 - von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen.

- **Intervenierbarkeit**
  Den Betroffenen werden die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt. Die verarbeitende Stelle ist verpflichtet, die entsprechenden Maßnahmen umzusetzen.

- **Transparenz**
  Sowohl Betroffene als auch die Betreiber von IKT-Systemen sowie zuständige Kontrollinstanzen können (in unterschiedlichem Maße) erkennen, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

  Transparenz bedeutet auch, dass personenbezogene Daten ihrem Ursprung gesichert zugeordnet werden können (Authentizität), und dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit).

6 Informationssicherheitsstrategie

Die Informationssicherheit wird im Land Berlin unter Einsatz und auf Grundlage der IT-Grundschutzmethodik des BSI gewährleistet.

6.1 ISMS-Prozess

Ziel der Informationssicherheitsstrategie des Landes Berlin ist es, mit wirtschaftlichem Ressourceneinsatz das erforderliche Maß an Sicherheit zu erreichen und verbleibende Restrisiken zu minimieren. Die Informationssicherheitsstrategie wird durch die Einführung eines Informations-Sicherheits-Management-Systems (ISMS) gemäß BSI-Standards realisiert, und als kontinuierlicher Prozess gestaltet.

Der Prozess umfasst die Schritte

- **Planung:** Festlegung der Vorgaben für den Sicherheitsprozess und das ISMS

- **Umsetzung:** Aufbau eines ISMS, Erstellung und Umsetzung eines Sicherheitskonzepts sowie Etablierung des Sicherheitsprozesses

- **Überprüfung:** kontinuierliche Erfolgskontrolle durch Nachweis der Wirksamkeit von Maßnahmen zur Erreichung der Sicherheitsziele

- **Aufrechterhaltung:** Durchführung von Korrekturen zur Optimierung des Sicherheitsprozesses und der Sicherheitsorganisation

Das ISMS wird gemäß § 21, Abs. 2 Satz 2 Nr. 4 EGovG Bln zentral gesteuert.

Alle Behörden der Berliner Verwaltung sind verpflichtet, ein Informations-Sicherheits-Management-System (ISMS) gemäß den Standards des BSI aufzubauen und weiterzuentwickeln (vgl. § 23 EGovG Bln).

Die Unterstützung des ISMS-Prozesses erfolgt mit dem in der IKT-Architektur festgesetzten Werkzeug (ISMS-Tool).

6.2 Grundsätze

Die Sicherheitsstrategie wird von den folgenden Grundsätzen der Informationssicherheit geprägt:

- **Sicherheit für nachhaltige Verfügbarkeit:** Um eine langfristige Verfügbarkeit zu erreichen, ist grundsätzlich eine kurzfristige Einschränkung bei Funktionalität und Komfort vertretbar.

- **Prinzip des Schutzbedarfs:** Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Daten und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Daten die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Der Schutzbedarf wird in die Kategorien "normal", "hoch" und "sehr hoch" eingeteilt. Bei hohem oder sehr hohem Schutzbedarf ist eine ergänzende Risikoanalyse nach den Standards des BSI erforderlich. Darauf aufbauend sind ggf. zusätzliche Maßnahmen notwendig.[6]

- **Minimalprinzip des Zugriffs:** Der Zugriff auf IKT-Systeme und Informationen wird auf die notwendigen Personen und Systeme beschränkt.

- **Einbindung aller Beschäftigten:** Alle Beschäftigten werden in den Sicherheitsmanagementprozess eingebunden und hinsichtlich der Informationssicherheit geschult und sensibilisiert. Sensibilisierungs- und Schulungsmaßnahmen für die Beschäftigten sind von herausgehobener Bedeutung und stellen eine permanente Aufgabe im Informationssicherheitsprozess dar. Eine regelmäßige Durchführung der notwendigen Maßnahmen ist (in Anlehnung an entsprechende Regelungen im Arbeits- und Gesundheitsschutz) zu gewährleisten.

- **Zentrale Rolle der Informationssicherheit:** Die Informationssicherheit wird bei Änderungen und Neuerungen im Verwaltungshandeln von Beginn an mit berücksichtigt. Der oder die Beauftragte für Informationssicherheit ist bei allen Fragen zur Informationsverarbeitung zu beteiligen und zu unterstützen.

[6] Näheres regelt eine Richtlinie zur Risikoanalyse.

- **Verhältnismäßigkeit der Sicherheitsmaßnahmen:** Aufwand und Ergebnis der eingesetzten Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen. Das Ergebnis der Abwägung ist zu dokumentieren.

- **Notfallmanagement:** Das Notfallmanagement bzw. die Notfallvorsorge ist integraler Bestandteil des ISMS-Prozesses und auf Basis regelmäßiger Notfallübungen zu überprüfen. Näheres regelt eine Richtlinie zum Notfallmanagement

- **Risikomanagement:** Das Risikomanagement umfasst die Identifikation und Bewertung von Risiken sowie die Durchsetzung von Mechanismen, um mit diesen effektiv umzugehen. Ziel ist es u. a., Gefährdungen und Sicherheitsvorfälle realistisch zu bewerten und hieraus Rahmenbedingungen für angemessene Aktionen abzuleiten.[7] Das Risikomanagement hat ggf. die Ergebnisse einer Datenschutzfolgeabschätzung zu berücksichtigen.

  Erkannte Risiken sind hinsichtlich ihrer Auswirkungen auf die sichere Wahrnehmung der Fachaufgaben und der Gewährleistung des Informationellen Selbstbestimmungsrechts (Datenschutz) zu bewerten. Die abschließende Entscheidung über die Tragbarkeit von Risiken trägt die Behördenleitung. Solange untragbare Risiken nicht durch geeignete Maßnahmen auf ein tragbares Maß reduziert werden können, ist auf den IKT-Einsatz (temporär) zu verzichten bzw. ist dieser einzuschränken. Die Entscheidung obliegt grundsätzlich der Behördenleitung (unter Beachtung der Verantwortung des ITDZ und der zentralen IKT-Steuerung gemäß Tz. 7.7).

  Untragbare Risiken für das informationelle Selbstbestimmungsrecht dürfen auch eingeschränkt nicht eingegangen werden.

6.3 IT-Sicherheitskonzepte

Für die im Land Berlin genutzte IKT sind IT-Sicherheitskonzepte (IT-SiKo) nach den BSI-Standards[8] 100-1 und 100-2 unter Berücksichtigung der Standards 100-3 und 100-4 zu erstellen und regelmäßig im Rahmen des ISMS-Prozesses weiter zu entwickeln und zu aktualisieren. IT-Sicherheitskonzepte sind in folgenden Ausprägungen erforderlich:

A) Behördenbezogene IT-Sicherheitskonzepte in Verantwortung der jeweiligen Behörde.
Sie umfassen die behördenbezogenen übergreifenden und nicht bereits durch die Standard-IKT-Sicherheitsbausteine für die

---

[7] Eine explizite Risikoanalyse ist gemäß BSI-Standards nur erforderlich, sofern der Schutzbedarf höher als normal ist.

8 Die BSI-Standards werden derzeit im Rahmen der Modernisierung des IT-Grundschutzes fortgeschrieben und zukünftig als Standard 200-x geführt. Die Übergangsfristen zwischen gegenwärtig gültigem und dem modernisierten IT Grundschutz ergeben sich aus den Vorgaben des BSI.

verfahrensunabhängige IKT-Infrastruktur abgedeckten Komponenten des IT-Grundschutzes.

B) **Verfahrensbezogene IT-Sicherheitskonzepte** für jedes IT-Fachverfahren in Verantwortung des oder der jeweiligen IT-Fachverfahrensverantwortlichen.

C) **IT-Sicherheitskonzepte für IKT-Basisdienste** in Verantwortung des jeweiligen Betreibers der IKT-Basisdienste.

D) **Standard-IKT-Sicherheitsbausteine für die verfahrensunabhängige IKT-Infrastruktur** werden vom ITDZ Berlin erstellt und umgesetzt. Sie sind auch für Behörden verbindlich, deren verfahrensunabhängige IKT-Infrastruktur noch nicht vom ITDZ Berlin betrieben wird. Die Umsetzung der in den Standard-IKT-Sicherheitsbausteinen definierten Maßnahmen obliegt in diesem Fall ebenfalls den jeweiligen Behörden.

In allen IT-SiKo sind die ggf. bestehenden Schnittstellen zu anderen IT-SiKo konkret zu beschreiben, wobei referenzierte Maßnahmen nachvollziehbar adressiert werden, so dass eine Prüfung möglich ist. In den verfahrensbezogenen IT-SiKo sind (zumindest bei hohem Schutzbedarf) die IT-Sicherheitsanforderungen an IKT-Basisdienste, verfahrensunabhängige IKT-Infrastruktur und weitere behördenbezogene Komponenten (behördenbezogenes IT-SiKo) darzustellen und die Einhaltung dieser IT-Sicherheitsanforderungen geeignet nachzuweisen. Sofern bestehende IT-Sicherheitsanforderungen nicht ausreichend durch diese referenzierten IT-SiKos abgedeckt werden, sind entsprechende verfahrensspezifische IT-Sicherheitsmaßnahmen erforderlich. Bei wesentlichen Änderungen der referenzierten Elemente ist seitens der IT-Fachverfahrensverantwortlichen zu prüfen, ob die definierten Sicherheitsanforderungen weiterhin erfüllt werden und ggf. ergänzende verfahrensspezifische Sicherheitsmaßnahmen erforderlich sind. Umgekehrt sind die bei einer Einführung von neuen IT-Fachverfahren (oder ihrer wesentlichen Änderung) entstehenden neuen Risiken zu benennen und deren ausreichende Minderung durch die in den o. a. anderen IT-SiKo festgelegten Maßnahmen zu prüfen.

6.4 Datenschutz

Der Datenschutz personenbezogener Daten ist integraler Bestandteil der Informationssicherheit. Datenschutz kann ohne Informationssicherheit nicht verwirklicht werden.

Der Datenschutz ist insbesondere bei der Erstellung von verfahrensbezogenen IT-Sicherheitskonzepten für Verfahren, die personenbezogene Daten entsprechend der Begriffsdefinition des Berliner Datenschutzgesetzes (BlnDSG) verarbeiten, zu berücksichtigen und entsprechende Maßnahmen sind umzusetzen. Dabei sind die zur Umsetzung datenschutzrechtlicher Anforderungen erforderlichen technischen und organisatorischen IT-

Sicherheitsmaßnahmen in den jeweiligen IT-Sicherheitskonzepten in geeigneter Weise auszuweisen[9].

6.5 Notfallmanagement

Ziel des Notfallmanagements ist es, sicherzustellen, dass die Geschäftsprozesse der Verwaltung selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die Aufgabenwahrnehmung auch bei einem größeren Schadensereignis gesichert bleibt. Eine ganzheitliche Betrachtung ist daher ausschlaggebend. Es sind alle Aspekte zu betrachten, die zur Fortführung der Geschäftsprozesse bei Eintritt eines notfallverursachenden Schadensereignisses erforderlich sind, nicht nur die Ressource Informationstechnik. Die Verantwortung für ein Notfallmanagement ist auf der obersten Leitungsebene der Behörde zu etablieren. Diese ist verantwortlich dafür, dass Risiken erkannt, reduziert und die Auswirkungen auf die Behörde bei Eintreten eines Schadensereignisses minimiert werden.

Das behördliche Notfallmanagement wird von einem oder einer Notfallbeauftragten gesteuert. Die Durchführung regelmäßiger behördlicher Notfallübungen ist sicherzustellen.

Der oder die Landesbeauftragte für Informationssicherheit steuert das behördenübergreifende Notfallmanagement.

Näheres regelt eine Richtlinie zum Notfallmanagement[10].

7 Organisationsstruktur für Informationssicherheit

Die Organisationsstruktur für die Informationssicherheit der vom Geltungsbereich des EGovG Bln erfassten Einrichtungen der Berliner Verwaltung besteht aus den folgenden Rollen, deren Aufgaben nachfolgend weiter ausgeführt sind:

- die IKT-Staatssekretärin oder der IKT-Staatssekretär
- die oder der Landesbeauftragte für Informationssicherheit (Landes-InfSiBe)
- das Berlin-CERT
- das IT-Dienstleistungszentrum Berlin (ITDZ Berlin) in seiner Rolle als Betreiber der verfahrensunabhängigen IKT-Infrastruktur
- das Informationssicherheitsmanagement-Team (InfSiMa-Team)

9 Das Sicherheitskonzept i. S. v. § 5 Abs. 3 BlnDSG besteht aus dem oder den verfahrensbezogenen IT-Sicherheitskonzepten der Fachverfahren, die für eine Verarbeitung personenbezogener Daten vorgesehen sind, sowie der relevanten Teile aller Sicherheitskonzepte von Basisdiensten, verfahrensunabhängiger IKT-Infrastruktur und behördenbezogener verfahrensabhängiger IKT, die im Rahmen der Datenverarbeitung zum Einsatz kommt. Entsprechendes gilt für die Datenverarbeitung, die ausschließlich in verfahrensunabhängiger IKT stattfindet.

10 Diese Richtlinie wird nach der Festsetzung der InfoSic-LL kurzfristig erstellt.

- die AG Informationssicherheit
- die behördlichen Informationssicherheitsbeauftragten (beh-InfSiBe)
- die IT-Fachverfahrensverantwortlichen

Weitere Rollen und Gremien können bei Bedarf in die Organisationsstruktur eingebunden werden.

Bei der Besetzung der Rollen wird darauf geachtet, dass die Personen fachlich und persönlich für die ihnen zugewiesene Aufgabe qualifiziert sind bzw. werden.

7.1 IKT-Staatssekretärin oder IKT-Staatssekretär

Der IKT-Staatssekretär oder die IKT-Staatssekretärin hat die Gesamtverantwortung für die Informationssicherheit in der Berliner Verwaltung und steuert den behördenübergreifenden Informationssicherheitsprozess. Dazu gehört insbesondere die fortlaufende Weiterentwicklung und Festsetzung der zentralen IKT-Sicherheitsarchitektur und der Standards für die IKT-Sicherheit in der Berliner Verwaltung und deren Unterstützung und Überwachung bei der Umsetzung der IKT-Sicherheits-Standards gemäß § 21, Abs. 2 Satz 2 Nr. 4 EGovG Bln.

Der IKT-Staatssekretär oder die IKT-Staatssekretärin kann diese Aufgaben an einen Bevollmächtigten oder eine Bevollmächtigte aus seiner oder ihrer Organisationseinheit übertragen.

Die IKT-Sicherheitsarchitektur umfasst

- die Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin (InfoSic-LL),
- Methodische und technisch-organisatorische Richtlinien zu einzelnen Aspekten der IKT-Sicherheit, die die InfoSic-LL durch Vorgabe standardisierter Rahmenbedingungen für wesentliche Aspekte der IKT-Sicherheit konkretisieren,
- IKT-Basisdienste für IKT-Sicherheit, die gemäß § 24 EGovG Bln vom ITDZ Berlin den Behörden zur verbindlichen Nutzung bereitgestellt werden sowie
- Standard-IKT-Sicherheitsbausteine für die verfahrensunabhängige IKT

und definiert in diesem Sinne auch die IKT-Sicherheits-Standards[11].

[11] Näheres regelt das Rahmendokument „IKT-Sicherheitsarchitektur des Landes Berlin“.

7.2 Landesbeauftragter oder Landesbeauftragte für Informationssicherheit (Landes-InfSiBe)

Der oder die Landesbeauftragte für Informationssicherheit verantwortet die operativen Einzelaufgaben zur Umsetzung von § 21 Abs. 2 Satz 2 Nr. 4 EGovG Bln.

Der oder die Landes-InfSiBe ist bei der von dem IKT-Staatssekretär oder der IKT-Staatssekretärin geleiteten Organisationseinheit gemäß § 21 Abs. 1 Satz 2 EGovG Bln angesiedelt.

Er oder sie hat ein direktes Vortragsrecht bei dem IKT-Staatssekretär oder der IKT-Staatssekretärin.

Zu den Aufgaben des oder der Landes-InfSiBe gehören insbesondere:

- operative Steuerung des behördenübergreifenden Informationssicherheitsprozesses,
- Erstellung der zentralen IKT-Sicherheitsarchitektur mit den Standards für die IKT-Sicherheit sowie weiterer Richtlinien zur Informationssicherheit,
- Definition von IKT-Basisdiensten zur Informationssicherheit,
- Überwachung der Umsetzung der IKT-Sicherheitsarchitektur und IKT-Sicherheits-Standards,
- Regelmäßige Berichterstattung über den Stand der Informationssicherheit,
- Unterstützung der Behörden bei der Umsetzung der IKT-Sicherheits-Standards,
- Fachliche Steuerung des ITDZ bzgl. der Informationssicherheit.

7.3 Behördliche Informationssicherheitsbeauftragte (beh-InfSiBe)

Die beh-InfSiBe initiieren, steuern, koordinieren und kontrollieren den Informationssicherheitsprozess in ihren Geschäftsbereichen. Sie haben ein direktes Vortragsrecht bei der Leitung ihrer Behörde.

In größeren Behörden bzw. komplexen Geschäftsbereichen erhalten die beh-InfSiBe bei Bedarf Unterstützung durch ein Informationssicherheitsmanagement-Team (ISM-Team) ihrer Behörde.

Sie unterstützen den oder die Landes-InfSiBe in allen Fragen der Informationssicherheit.

7.4 Das Berlin-CERT

Das ITDZ Berlin betreibt zur Unterstützung und Beratung der Behörden der Berliner Verwaltung bei sicherheitsrelevanten Vorfällen in IKT-Systemen ein Computersicherheits-Ereignis- und Reaktionsteam (Berlin-CERT) unabhängig von den sonstigen betrieblichen Aufgaben des ITDZ Berlin. Die an das Berliner Landesnetz angeschlossenen Behörden und Einrichtungen haben dem Berlin-CERT sicherheitsrelevante Vorfälle unverzüglich zu melden.

Die Aufgaben des Berlin-CERT untergliedern sich wie folgt:

- präventiv
  - Annahme und regelmäßige Verteilung sicherheitsrelevanter Informationen und Empfehlungen (Warn- und Informationsdienst)
  - frühzeitige Erkennung von Angriffen oder Missbrauch
- reaktiv
  - Bearbeitung und Dokumentation von Anfragen zu erkannten IT-Sicherheitsvorfällen
  - Unterstützung bei der Reaktion auf Vorfälle
  - Koordination der notwendigen Maßnahmen zur Bewältigung ressortübergreifender IT-Sicherheitsvorfälle
- verbessernd
  - Durchführung von Sensibilisierungs- und Schulungsmaßnehmen zu Themen der IKT-Sicherheit
- organisatorisch
  - Kontaktstelle und Ansprechpartner für die Zielgruppen im Land Berlin sowie in der Außenvertretung zu anderen CERT- und IT-Sicherheitsorganisationen

7.5 Informationssicherheitsmanagement-Team (InfSiMa-Team)

Das Informationssicherheitsmanagement-Team (InfSiMa-Team) berät den Landesbeauftragten oder die Landesbeauftragte für Informationssicherheit zu strategischen oder behördenübergreifenden Aspekten der Informationssicherheit. Es besteht aus

- dem oder der Landesbeauftragten für Informationssicherheit (Vorsitz)
- den Behördlichen Informationssicherheitsbeauftragten
- dem oder der Informationssicherheitsbeauftragten des ITDZ Berlin

Darüber hinaus können weitere Teilnehmerinnen und Teilnehmer hinzugezogen werden. Den Informationssicherheitsbeauftragten der Verwaltung des Abgeordnetenhauses, des Rechnungshofs von Berlin und der Beauftragten für Datenschutz und Informationsfreiheit steht die Teilnahme frei.

Das InfSiMa-Team tagt in der Regel zweimal im Jahr.

7.6 AG Informationssicherheit (AG InfoSic)

Die AG InfoSic berät das ITDZ Berlin zu technisch-operativen Aspekten der Informationssicherheit, insbesondere bzgl. der Sicherheitsmaßnahmen für die verfahrensunabhängige IKT.

Die AG InfoSic wird vom ITDZ geleitet. Die konkrete Besetzung der AG InfoSic wird vom ITDZ mit den Behörden abgestimmt. Die zentrale IKT-Steuerung nimmt an den Sitzungen teil.

7.7 IT-Dienstleistungszentrum Berlin (ITDZ Berlin)

Das ITDZ Berlin ist der zentrale Dienstleister für die IKT-Sicherheit der Berliner Verwaltung. Im ITDZ Berlin wird ein ISMS gemäß den Standards des BSI umgesetzt.

Sofern das ITDZ Berlin nach § 24 Abs. 2 EGovG Bln die verfahrensunabhängige IKT-Infrastruktur bereitstellt bzw. betreibt, obliegt dem ITDZ Berlin die (Umsetzungs-)Verantwortung hinsichtlich der IKT-Sicherheit für die entsprechenden Komponenten.

Bei schwerwiegenden und akuten Gefährdungen für die Informationssicherheit der Berliner Verwaltung, bei denen gravierende Auswirkungen auf die sichere Aufgabenwahrnehmung von Teilen oder insgesamt der Berliner Verwaltung zu erwarten sind, hat das ITDZ das Recht, auf Empfehlung des Berlin-CERT und nach Zustimmung durch den oder die Landes-InfSiBe sowie - soweit möglich –- in Abstimmung mit der oder dem beh-InfSiBe der ggf. betroffenen Einrichtung Zugänge zum Berliner Landesnetz oder den Übergang ins Internet temporär einzuschränken oder zu sperren, sofern davon auszugehen ist, dass ein voraussichtlich gravierender Schaden nicht anders abgewendet werden kann.

7.8 IT-Fachverfahrensverantwortliche

Sicherheitsanforderungen an die verfahrensabhängige IKT werden von der IKT-Staatssekretärin oder dem IKT-Staatssekretär in enger Zusammenarbeit mit der jeweils zuständigen Fachverwaltung definiert (§ 21, Abs. 2 Satz 2 Nr. 9 EGovG Bln). Sie basieren auf der IKT-Sicherheitsarchitektur und konkretisieren diese für die IT-Fachverfahren.

Die IT-Fachverfahrensverantwortlichen verantworten die Umsetzung dieser Anforderungen in den jeweiligen verfahrensbezogenen IT-Sicherheitskonzepten gemäß Tz. 6.3.

8 Erfolgskontrolle

Der IKT-Staatssekretär oder die IKT-Staatssekretärin überwacht die Umsetzung der IKT-Sicherheitsarchitektur und kann dazu von Behörden entsprechende Unterlagen, insbesondere IT-Sicherheitskonzepte abfordern.

Das dezentrale ISMS gemäß § 23 EGovG Bln ist regelmäßig auf seine Aktualität und Wirksamkeit zu prüfen. Dabei sind die Maßnahmen auch daraufhin zu untersuchen, ob sie den betroffenen Beschäftigten bekannt, umsetzbar, in den Betriebsablauf integrierbar und wirksam sind.

Jede Behörde erstellt mindestens einmal jährlich einen behördlichen Bericht zur Informationssicherheit. Der Bericht wird der Behördenleitung vorgelegt.

Die behördlichen Berichte werden nach Billigung durch die jeweilige Behördenleitung der oder dem Landes-InfSiBe übermittelt. Der oder die Landes-InfSiBe hat das Recht, die Angaben in geeigneter Weise zu überprüfen.

Der oder die Landes-InfSiBe erstellt auf dieser Basis jährlich einen landesweiten „Bericht zur Informationssicherheit im Land Berlin“.

Zur Erstellung der Berichte wird ein landesweit einheitliches Modell genutzt.

9 Verstöße und Folgen

Werden Verstöße gegen die Vorgaben dieser Leitlinie oder darauf aufbauender Regelungen festgestellt, so wird die betreffende Einrichtung über den oder die Landes-InfSiBe aufgefordert, in einer angemessenen Frist die Vorgaben umzusetzen.

Bei anhaltenden Verstößen gegen die Vorgaben eskaliert der oder die Landes-InfSiBe den Vorfall an den IKT-Staatssekretär oder die IKT-Staatssekretärin.

Ist die Verarbeitung personenbezogener Daten betroffen, so ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit zu benachrichtigen.

10 Schlussbestimmungen

Diese Leitlinie zur Informationssicherheit tritt am 21.09.2017 in Kraft.

Im Rahmen des Informationssicherheitsprozesses wird diese Leitlinie zur Informationssicherheit regelmäßig (bei wesentlichen Änderungen von in der Leitlinie benannten Referenzdokumenten und mindestens alle zwei Jahre) auf ihre Aktualität hin überprüft und ggfs. aktualisiert.